ALESSA

CIPHERTRACE

Definitions, Obligations and Best Practices

What Banks Need to Know About Cryptocurrency

What is a cryptocurrency?

While often used interchangeably, virtual asset, virtual currency, and cryptocurrency each mean slightly different things. Digital currency is a broad term for any payment method that is in electronic form. A virtual currency is a subset of digital currency and is a digital representation of value, issued by private developers and denominated in their own unit of account. Virtual currency only exists in electronic form and is not tangible.

Cryptocurrency is a type of virtual currency that uses cryptographic protocols to secure the currency. Cryptocurrency bundles up transactions into blocks and uses various cryptographic protocols (based on the individual cryptocurrency) to establish the correctness and permanence of each block. After the block is verified, it is added to the end of a blockchain.

While these terms differ slightly, from a regulatory compliance perspective, they can be treated as one-and-the-same, as many people, and some regulators, use these terms interchangeably and they require similar due diligence when evaluating the risks associated with each.

What Do Regulators Call It?

- Financial Crimes Enforcement Network (FinCEN) – “Convertible Virtual Currency” (CVC)
- U.S. Commodity Futures Trading Commission (CFTC) – “Digital Asset”
- Financial Action Task Force (FATF) – “Virtual Asset”
- EU AMLD – “Virtual Currency”
- SEC – “Digital Asset”

Must-*K*now Cryptocurrency *B*usinesses

Along with the advent of cryptocurrency, there has been the creation of new types of businesses that financial markets have never seen before. Collectively referred to as Virtual Asset Service Providers (VASPs, these include cryptocurrency exchanges, digital wallets, custodial services, and Bitcoin ATMs.

The Financial Action Task Force (FATF), the global money laundering and terrorist financing watchdog, classifies "virtual asset service provider" as any natural or legal person who is not covered elsewhere under their Recommendations and, as a business, conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

- Exchange between virtual assets and fiat currencies
- Exchange between one or more forms of virtual currencies
- Transfer of virtual assets
- Safekeeping or administration of virtual assets, known as custody providers
- Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual currency known as Initial Coin Offerings (ICOs) and Security Token Offerings (STOs)

Fiat-to-Crypto Exchange

Fiat-to-Crypto exchanges provide users the ability to exchange fiat currency (USD, EUR, CAD, etc.) for cryptocurrency. These exchanges allow users to send and receive cryptocurrency and make deposits and withdrawals in fiat currency. In many jurisdictions, fiat-to-crypto exchanges must be registered with their local Financial Intelligence Unit (FIU) as a money services business (MSB). Because these exchanges are a prime off-ramp from the virtual to the fiat world, they can often be targeted by bad actors seeking to launder their ill-gotten funds.

Crypto-to-Crypto Exchange

Some exchanges do not provide direct access to fiat currencies, but rather serve as a method to exchange one type of cryptocurrency for another. These exchanges often provide access to a greater number of cryptocurrencies.

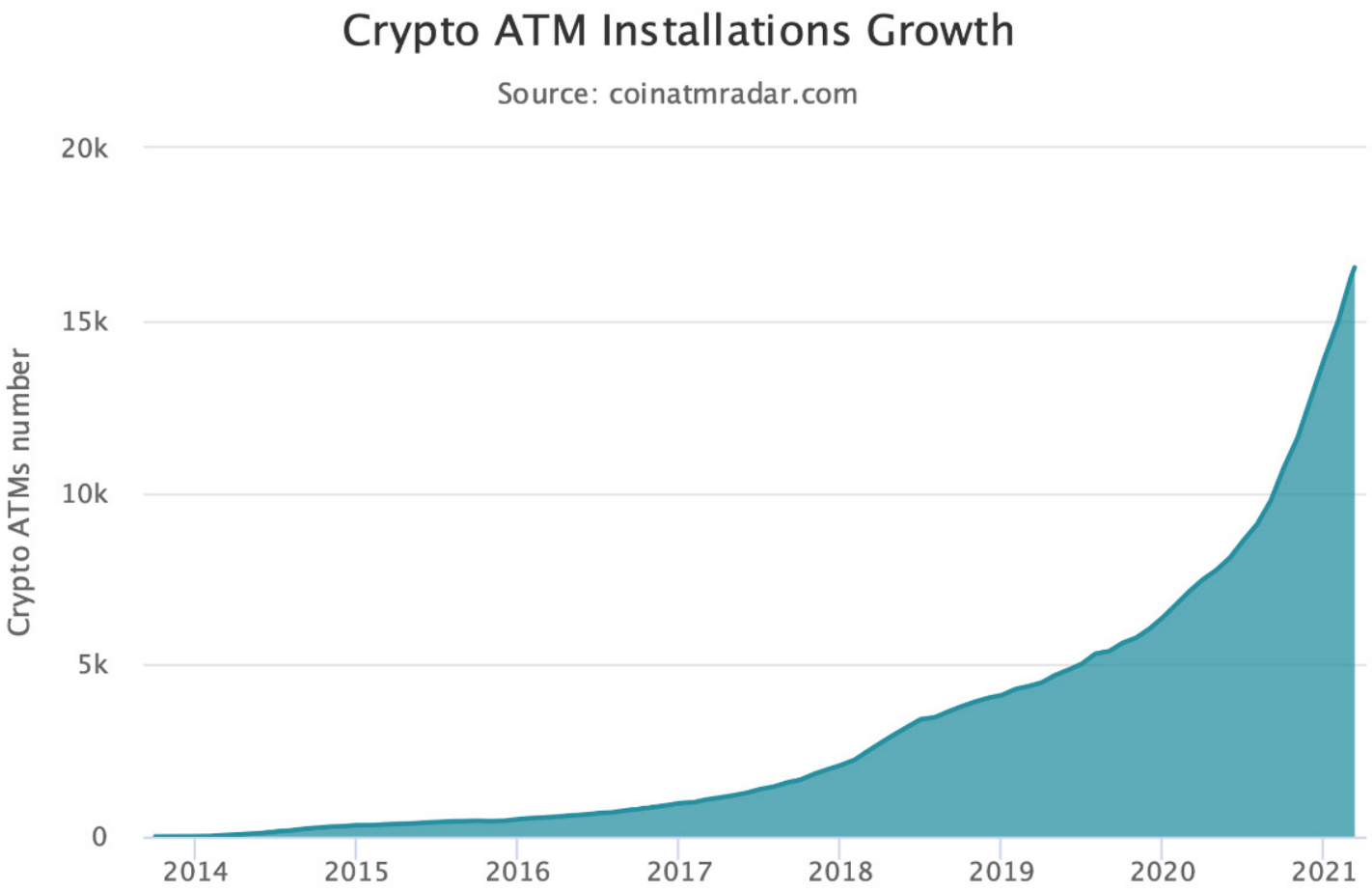
These crypto-to-crypto exchanges are not covered by AML regulations in certain jurisdictions, such as AMLD5 in the EU, and will often have weaker know your customer (KYC) practices than a fiat-to-crypto exchange. While they are not used as a fiat off-ramp, crypto-to-crypto exchanges can be used to obfuscate the flow of funds from blockchain analytics, requiring law enforcement to subpoena the exchange for additional transactional information before an investigation can continue. While less risky, many of these exchange trade anonymity-enhanced currencies (AECs), creating different risks.

Cryptocurrency Kiosks

Crytpocurrency Kioks—or Bitcoin ATMs (BATMs)— allow users to purchase cryptocurrency with cash or bank cards and new retail locations are easily installed. According to data from coinatmradar.com, the number of new BATMs has grown exponentially over the past few years, with 16,529 BATMs worldwide by March 2021. More than half of these kiosks are located in the United States.

Custodial Services

While cryptocurrency provides users the ability to store their private keys, many users choose to use a service to store their keys. Centralized exchanges provide this feature for their users as do a number of online wallet services. As these services hold and transmit funds, they often have to register with appropriate FIUs as MSBs.



While Bitcoin ATMs require MSB license in the US, they remain unregulated in many jurisdictions.

As cryptocurrency and blockchain adoption around the world continues to accelerate, more and more traditional financial institutions are looking to introduce crypto into their services. On February 11, 2021, America's oldest bank, BNY Mellon, announced their plan to custody cryptocurrencies on behalf of its clients. The impetus for the decision reportedly came from institutional investors amid the 2021 bull season for the asset class.

BNY was just the latest of multiple financial institutions that have added crypto custody to their services. PayPal announced that the company would add crypto buying, selling, and custody features to "Venmo and select international markets" in 2021.

Decentralized Exchanges (DEX)

Decentralized, or peer-to-peer (P2P) exchanges do not use a central authority to facilitate transactions and do not store any cryptocurrency on local servers. Rather, they serve as a means of connecting buyers and sellers who then transact directly or through proxy tokens. Most DEXs do not currently provide for any registration, KYC or anti-money laundering compliance.

Despite these decentralized identities, it appears regulators are beginning to pay closer attention to DEXs and their compliance requirements while serving customers in their jurisdictions.

FATF already considers DEXs to be VASPs and FinCEN applies the same regulatory consideration to DEXs that it does to bitcoin ATMs— when they perform money transmission, the definition of money transmitter will apply to the owner/operator, regardless of whether or not they operate for profit.

Other Digital Asset Companies

With an industry as large as cryptocurrency, there are many other types of businesses that may come into contact with traditional FIs. Each one may represent unique risks and may or may not have a similar counterpart in traditional markets. These include peer-to-peer lending services, Over-the-Counter (OTC) trading platforms, gambling services and investment funds.

ICOs (Initial Coin Offerings) and STOs (Security Token Offerings) are both mechanisms for businesses to raise money through the issuance of digital tokens. Those tokens can represent a utility such as a pre-purchase of a product (ICO) or a security (STO). In 2018 almost $8 billion was raised through ICOs and STOs.

As part of their overall risk-based approach to cryptocurrencies, financial institutions must understand the type of business when determining whether to onboard the business as a client and/or whether to transact with that business. For example, Mixing Services are a type of VASP that serves to obfuscate the transaction source or destination. These are high-risk businesses that are frequently used to launder money through the blockchain.

Cryptocurrency AML Obligations

While many traditional banks and other financial services businesses have taken a wait-and-see approach, the explosive growth of this industry coupled with regulatory push is requiring these institutions to take a more active role in identifying the risks associated with cryptocurrency transactions and businesses.

For those financial institutions looking to monetize on the opportunities presented, there is the challenge on how best to enter the cryptocurrency market while still maintaining a risk-based approach towards regulatory compliance.

While the extent of regulation for certain cryptocurrency transactions and crypto-to-crypto exchanges differs by jurisdiction, one thing is clear—most countries seem to agree that the commercial exchange of cryptocurrency for fiat currency should be subject to KYC, AML, and securities obligations.

FinCEN perspective

FinCEN (and many other regulators) classifies most virtual asset service providers as MSBs, which are required to register with the agency ad comply with the AML regulations under the Bank Secrecy Act (BSA).

Existing FinCEN regulations and advisories clearly state that it is the responsibility of all financial institutions to identify and report suspicious activity concerning how criminals and other bad actors exploit virtual currency for money laundering, sanctions evasion, and other illicit financing purposes. FinCEN continues to emphasize that these requirements apply to all financial institutions, even if those financial institutions do not directly buy, sell, or provide custody to virtual assets or bank VASPs.

For financial institutions looking to bank VASPs, consider the following when having conversations with legal counsel:

"…banks must be thinking about their crypto exposure as well. These are areas your examiners, and FinCEN, will ask you about when assessing the effectiveness of your AML program… If banks are not thinking about these issues, it will be apparent when examiners visit."

- FinCEN Director Blanco, September 29, 2020

- **Cryptocurrency Exchanges and Bitcoin ATM** providers, must register as an MSB and comply with the BSA including having a complete AML program. **Hosted wallet and custody** services must comply fully with BSA requirements. Unhosted wallet providers, such as deployed software or most hardware wallets, are not required to comply with BSA and FinCEN AML requirements.
- **Cryptocurrency Payment Processors** (also known as fiat gateways) do not qualify for the BSA exemptions provided to fiat payment processors as they may process payments from individual wallets, unlike fiat payment processors who only process payments from financial institutions through credit card payments or bank transfers. Because of this, cryptocurrency payment processors must comply with BSA and FinCEN AML requirements.
- **Token Offerings** (Initial Coin Offerings, Initial Exchange Offerings, Security Token Offerings, et al) provide the most complex scenarios for determining AML/BSA requirements. These types of institutions have different AML/BSA requirements and will differ from those of an MSB.
- **Travel Rule Compliance** is required by all U.S. financial institutions though was seldom enforced in the crypto space. However, in 2020, FinCEN decidedly refocused on the regulation by proposing several new rules for crypto payments. These proposed rules would explicitly apply the Travel Rule to U.S. exchanges, trading desks, ATMs and custody providers.

Why bank VASPs?

Virtual asset service providers can be higher risk, but they can also be very lucrative customers. As of January 2020, Coinbase, a U.S. cryptocurrency exchange, oversaw $21B in assets for 35 million users who buy and sell cryptocurrency by connecting their bank accounts to their Coinbase accounts and is on track to be the first U.S. exchange to go public.

Examples of Crypto Risk Exposure

Cryptocurrency touches almost all banks, even banks not looking to onboard or bank businesses involved with cryptocurrencies. All financial institutions must be able to understand and identify their crypto risk exposure.

Extensive research in 2019 by the cryptocurrency intelligence company CipherTrace uncovered individuals operating illicit crypto MSBs at eight of ten U.S. retail banks. These illegal MSBs use their demand deposit accounts (DDA) as a conduit for accepting cash payments in exchange for cryptocurrency to support the illegal trade of fiat currency for crypto or digital currency. They often do this by a simple ACH transfer, wire transfer, or counter cash deposit at a depository institution.

Another scheme seen by financial institutions include peer-to-peer (P2P) crypto marketplaces. These exchangers help people buy and sell cryptocurrencies with in-branch cash deposits or discrete wire transfers. To conceal these unregistered MSBs, buyers are told not to inform bank tellers that they are making deposits for the purchase of bitcoin, but rather are purchasing “digital services.”

Similarly, for wire transfers, customers looking to buy bitcoin are directed to avoid mentioning “bitcoin” in any communication. In addition to being unregistered, many of these P2P exchangers lack any kind of AML program and perform little or no know your customer (KYC) due diligence. This lack of controls presents huge, hidden AML risks to banks and other financial institutions.

To help financial institutions identify risks, FinCEN has released a number of red flag indicators. They include the following:

Indicators Darknet Marketplaces

- A customer conducts transactions with CVC addresses that have been linked to darknet marketplaces or other illicit activity.
- A customer’s CVC address appears on public forums associated with illegal activity.
- A customer’s transactions are initiated from IP addresses associated with Tor.

- Blockchain analytics indicate that the wallet transferring CVC to the exchange has a suspicious source or sources of funds, such as a darknet marketplace.
- A transaction makes use of mixing and tumbling services, suggesting an intent to obscure the flow of illicit funds between known wallet addresses and darknet marketplaces

Unregistered or Illicitly Operating P2P Exchangers

- Transfers or receives funds, including through traditional banking systems, to or from an unregistered foreign CVC exchange or other MSB with no relation to where the customer lives or conducts business
- Utilizes a CVC exchanger or foreign-located MSB in a high-risk jurisdiction lacking, or known to have inadequate AML/CFT regulations for CVC entities, including inadequate KYC or customer due diligence measures
- A customer directs large numbers of CVC transactions to CVC entities in jurisdictions with reputations for being tax havens
- A customer that has not identified itself to the exchange, or registered with FinCEN, as a money transmitter appears to be using the liquidity provided by the exchange to execute large numbers of offsetting transactions

Unregistered Foreign MSBs

- Receives multiple cash deposits or wires from disparate jurisdictions, branches of a financial institution, or persons and shortly thereafter uses such funds to acquire virtual currency
- Receives a series of deposits from disparate sources that, in aggregate, amount to nearly identical aggregate funds transfers to a known virtual currency exchange platform within a short period of time.
- Customer's phone number or email address is connected to a known CVC P2P exchange platform advertising exchange services
- Transfers or receives funds, including through traditional banking systems, to or from an unregistered foreign CVC exchange or other MSB with no relation to where the customer lives or conducts business
- A customer utilizes a CVC exchanger or foreign-located MSB in a high-risk jurisdiction lacking, or known to have inadequate AML/CFT regulations for CVC entities, including inadequate KYC or customer due diligence measures
- A customer directs large numbers of CVC transactions to CVC entities in jurisdictions with reputations for being tax havens
- A customer that has not identified itself to the exchange, or registered with FinCEN, as a money transmitter appears to be using the liquidity provided by the exchange to execute large numbers of offsetting transactions,

Unregistered or Illicitly Operating CVC Kiosks

- A customer operates multiple CVC kiosks in locations that have a relatively high incidence of criminal activity.
- Large numbers of transactions from different customers sent to and from the same CVC wallet address but not operating as a known CVC exchange
- Structuring of transactions just beneath the CTR threshold or the CVC kiosk daily limit to the same wallet address either by using multiple machines or tied to the same phone number

Other Potentially Illicit Activity

- A customer conducts transactions with CVC addresses that have been linked to extortion, ransomware, sanctioned CVC addresses, or other illicit activity
- A customer's transactions are initiated from non-trusted IP addresses, IP addresses from sanctioned jurisdictions, or IP addresses previously flagged as suspicious
- Use of virtual private network (VPN) services or Tor to access CVC exchange accounts.
- A customer initiates multiple rapid trades between multiple virtual currencies with no related purpose, which may be indicative of attempts to break the chain of custody on the respective blockchains or further obfuscate the transaction
- A customer provides identification or account credentials (e.g., non-standard password, IP address, or flash cookies) shared by another account
- A customer conducts transactions or rapidly executes multiple conversions between various types of different CVCs below relevant due diligence, recordkeeping, or reporting thresholds and then transfers the value off of the exchange
- Discrepancies arise between IP addresses associated with the customer's profile and the IP addresses from which transactions are being initiated.
- A customer significantly older than the average age of platform users opens an account and engages in large numbers of transactions, suggesting their potential role as a CVC money mule or a victim of elder financial exploitation
- A customer shows limited knowledge of CVC despite engagement in CVC transactions or activity, which may indicate a victim of a scam
- A customer declines requests for "know your customer" documents or inquiries regarding sources of funds
- A customer purchases large amounts of CVC not substantiated by available wealth or consistent with his or her historical financial profile, which may indicate money laundering, a money mule, or a victim of a scam
- A common wallet address is shared between accounts identified as belonging to two different customers
- Deposits into an account or CVC address significantly higher than ordinary with an unknown source of funds, followed by conversion to currency of legal tender, which may indicate theft of funds
- Multiple changes to email address and other contact information for an account or customer which may indicate an account takeover against a customer
- Use of language in CVC message fields indicative of the transactions being conducted in support of illicit activity or in the purchase of illicit goods, such as drugs or stolen credit card information

Big Risks, Big Penalties

In one of the most significant takedowns of a cryptocurrency-anonymizing service, Federal law enforcement authorities arrested Larry Dean Harmon of Akron, Ohio, for money laundering. Harmon's Helix "mixing" operation moved approximately $300 million in bitcoin.

The Department of Justice alleged that Helix had partnered with now-defunct underground marketplace AlphaBay, which was known for drug dealing and other illegal activities until it was shut down in 2017 by law enforcement.

FinCEN imposed a $60 million civil money penalty against Harmon, for violations of the Bank Secrecy Act (BSA) and its implementing regulations. By accepting and transmitting bitcoin through a variety of means, Harmon operated as an exchanger of convertible virtual currencies.

The agency also found that Harmon willfully violated the BSA's registration, program, and reporting requirements by failing to register as a MSB, failing to implement and maintain an effective anti-money laundering program, and failing to report suspicious activities.

FATF also released a report on Virtual Assets Red Flag Indicators. Meant to assist reporting entities including financial institutions (FIs), designated non-financial businesses and professions (DNFBPs), and VASPs, in an excellent resource and focused on indicators of money laundering for VASPs. The report is available on the FATF website or refer to this blog for a summary of the indicators.

In order for banks to detect any of the red flags indicated, it is necessary for them to be able to accurately identify and monitor all crypto-related transactions. Doing so will allow them to identify the following red flags listed by FATF like the ones below:

- Transactions by a customer involving more than one type of VA, despite additional transaction fees, and especially those VAs that provide higher anonymity, such as anonymity-enhanced cryptocurrency or privacy coins.
- Moving a VA that operates on a public, transparent blockchain, such as Bitcoin, to a centralized exchange and then immediately trading it for an AEC or privacy coin.
- Customers that operate as an unregistered/unlicensed VASP on peer-to-peer (P2P) exchange websites, particularly when there are concerns that the customers handle huge amount of VA transfers on a customer's behalf, and charge higher fees to its customer than transmission services offered by other exchanges. Use of bank accounts to facilitate these P2P transactions.
- Abnormal transactional activity (level and volume) of VAs cashed out at exchanges from P2P platform-associated wallets with no logical business explanation.
- VAs transferred to or from wallets that show previous patterns of activity associated with the use of VASPs that operate mixing or tumbling services or P2P platforms.
- Users entering the VASP platform having registered their Internet domain names through proxies or using domain name registrars (DNS) that suppress or redact the owners of the domains.
- Use of VAs whose design is not adequately documented, or that are linked to possible fraud or other tools aimed at implementing fraudulent schemes, such as Ponzi schemes.
- Receiving funds from or sending funds to VASPs whose CDD or know-your-customer (KYC) processes are demonstrably weak or non-existent.

Tips for How to Evolve Your AML Program

Regardless of whether you are intentionally banking VASPs, every regulated entity needs to evolve their AML program to demonstrate a risk-based approach towards cryptocurrency businesses and transactions. To start, have policies and procedures in place that help you answer the questions like the ones below:

Know Your Customer

- Are any of your new (or existing) customers a registered P2P exchange, crypto MSB, crypto kiosk or any other VASP?
- Are any VASPs using my institution to transfer funds?
- Are any VASPs registered (as required)?
- What are the procedures to investigate and verify any of the above?
- If you are banking VASPs, do they have an adequate KYC program in place?
- How do you risk profile any VASP clients?

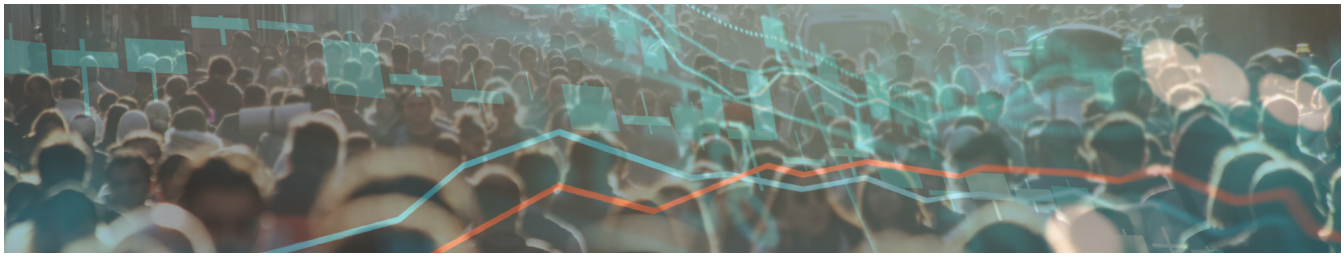
Transaction Monitoring

- Are virtual currency related transactions flowing through my institution? Are these valid transactions?
- Are there payments with a VASP?
- What is the purpose or source of wealth of any crypto transactions?
- Is the source suspicious or risky?
- Is the sender or receive an unlicensed MSB?
- If you are banking a VASP, are they able to identify the source and nature of the funds?

To help you answer some of the above questions, here are some tips for you to consider.

Avoid use of homegrown name-matching systems

Some financial institutions have built homegrown systems to try to identify cryptocurrency-related accounts, however, this approach results in many false positives and misses large amounts of funds flows. CipherTrace research has found that a typical name-based homegrown system may miss up to 70 percent or more of the crypto exchanges, and up to 90 percent of actual transaction volume.



For example, “Gemini” is not only associated with the famous crypto exchange run by the Winkelvoss twins, but also the Gemini Middle School in Maine, Gemini the “elite interior and exterior wood coating manufacturer,” Gemini the company “with 40+ years in the construction business,” and numerous other businesses. One can quickly see how name matching alone can result in a large number of false positives, waste valuable time and effort and still be ineffective.

Most open-source lists are incomplete, perhaps covering the top 100 exchanges, leaving out the other 600 plus exchanges. Even if customers were transacting with a cryptocurrency exchange you had on the list, many exchanges do not operate business under their popular name.

For example, cryptocurrency exchange “Zebitex” does business under the vague name “Digital Service,” while Abra’s legal name is “Plutus Financial Inc.” It is clear again that name matching is not sufficient to find all cryptocurrency exchanges and results in significant exposure.

Risk profile each VASP

Historically, financial institutions have treated all cryptocurrencies as one-and-the-same. This does not reflect the reality of cryptocurrency. Each cryptocurrency poses unique risk. As an example:

What is the level of privacy of the cryptocurrency?

Certain cryptocurrencies, provide significant privacy and anonymity for their users. Individuals use these currencies to ensure their transaction and account privacy. While this does not imply their activities are illicit or illegal, greater privacy implies greater risk for financial institutions. Understanding the different cryptocurrencies and their level of risk is as critical as and can be more difficult than understanding geopolitical risk.

What is the hacking risk of the cryptocurrency?

While established cryptocurrencies like Bitcoin and Ethereum have large networks that protect them from individuals or groups that may try to take over the currency, that is not the case for smaller currencies. Depending on the technical implementation, the market capitalization and the size of the network, certain cryptocurrencies may be easy to manipulate, potentially causing significant losses for its users.

Monitor for Crypto Transactions

As more mainstream consumer and institutional investors embrace cryptocurrencies, it becomes increasingly difficult, if not impossible, for traditional FIs to avoid entanglements with the crypto economy.

According to FinCEN, activity involving cryptocurrency may be observable by financial institutions specializing in:

- commerce related to crypto,
- financial institutions servicing such businesses, or
- financial institutions with customers actively involved in the use of cryptocurrency.

If a bank is unable to accurately determine if their institution is serving virtual asset businesses, or if their customers are transacting in virtual asset-related payments, there is no way for them to comply with their BSA obligations.

Use cryptocurrency intelligence tools

In 2021, bank examiners and FinCEN will focus on virtual currency exposure when assessing the effectiveness of bank AML programs. Traditional financial institutions must be able to identify institutional and peer-to-peer virtual currency-related transactions and understand how their institutions interact with emerging virtual asset service providers. Crypto-laundering risk mitigation for traditional financial institutions requires specialized tools to identify and report potentially suspicious activity.

Many digital asset entities obscure the nature of their business to avoid de-risking by banks. Unregistered MSBs and P2P schemes selling crypto for fiat using bank accounts frequently falsify Merchant Category Codes and provide incorrect industry details, making them challenging to detect.

Banks should supplement their AML programs with cryptocurrency intelligence that allow compliance teams to match payments to higher risk VASPs and peer-to-peer MSBs using legal identifiers, aliases and bank account numbers to produce the highest catch rate.

Without adequate intelligence, financial institution will be unable to detect most cryptocurrency-related activity on their credit cards, wire transfers and ACH transactions, resulting in a failure to adequately file Suspicious Activity Reports related to these transactions.

Use blockchain forensics

While blockchain technology provides new challenges for AML/BSA compliance, the public ledger of many cryptocurrencies such as Bitcoin or Ethereum allows for a level of transaction visibility that is not possible in traditional finance. Using blockchain forensics tools, compliance teams can analyze the transaction history and quickly risk rate any crypto customer or counterparty. This provides an incredibly valuable tool in analyzing the risk of an individual based on their transaction history and transaction proximity to high-risk wallets, such as dark markets.

Conclusion

The cryptocurrency market continues to grow and expand, with new businesses and cryptocurrency MSBs opening up almost daily. One third of all cryptocurrency exchanges have opened since the beginning of 2018, and this trend is unlikely to slow. With adoption of these new financial vehicles growing and new users coming on-board every day, financial institutions need to engage in this new industry while managing the associated risk.

When evaluating the risk associated with a particular cryptocurrency, compliance officers have new challenges and new risks to consider and manage.

1. As regulations across jurisdictions are still evolving, extra attention must be paid on what regulators require for compliance.
2. For those operating in the U.S., FinCEN has issued clarification for virtual asset providers and some types of businesses need to follow BSA and FinCEN AML requirements while others are exempt under special cases. Compliance officers should work with their legal counsel and directly with the regulators to understand their obligations.
3. Risk profile each cryptocurrency as each poses unique risk.
4. In addition to traditional transaction monitoring, institutions must monitor the transactions of their customers and other third parties on the blockchain. While the patterns may be similar between traditional finance and cryptocurrency, the methods used to identify these patterns are quite different.
5. Ensure all cryptocurrency businesses that they transact with meet industry standards for KYC and AML.
6. Watch for additional risks that are unique to cryptocurrency including the use of dark web marketplaces, mixing services and many others.
7. Supplement AML programs with cryptocurrency intelligence that match payments to higher risk VASPs and peer-to-peer MSBs.
8. Rely on technology that is designed to analyze blockchain transactions to mitigate risks associated with cryptocurrencies.

AML Compliance with Alessa

Alessa provides all the anti-money laundering (AML) capabilities that banks, money services businesses (MSBs), fintechs, casinos and other regulated industries need – all within one platform. Capabilities of the product include:

Due Diligence: To support KYC, CDD, and EDD processes, Alessa combines data from onboarding systems with identity verification and risk intelligence data to provide a risk score based on profile, activities and relationships.

Sanctions Screening: Alessa screens individuals and businesses against multiple lists including PEPs, negative news, OFAC, and other sanctions lists. Screening can be done in native characters and in real time, periodically or on demand.

Transaction Monitoring: Alessa analyzes every transaction in real-time and using advanced analytics, generates alerts for suspicious activities. These are directed to the appropriate personnel for investigation and/or reporting.

Regulatory Reporting: All suspicious activity alerts include data needed for regulatory reports. Once it is determined that a Suspicious Transaction Report or a Suspicious Activity Report needs to be filed, Alessa can auto-populate (and electronically file) as many as 70% of these reports. The solution can also automate as much as 100% of CTRs.

Risk Scoring: Alessa uses data from various sources to provide an assessment of the risks of doing business with an entity. The solution also periodically reviews an organization's customer base and updates their risk level based on their activity and third-party data.

Configurable: With Alessa, organizations can select the functionality they need or the complete solution. Permission-based functionality allows different users to access only the information they need, and data can be maintained in the cloud or on-premise, ensuring compliance with regulations.

Data Management: Alessa accesses data from any platform, including ERPs, bespoke applications, and core business systems. Better data means better insights.

Investigation Tools: Alessa offers dynamic workflows to guide processes and investigations. Enterprise search capabilities allow for easy searching of data within internal and external sources, while case management offers a collaborative approach to investigations, compliance, and decision-making.

Metrics & Insights: Alessa offers configurable dashboards that track key metrics and allow staff to drill down into the alerts and make decisions based on comprehensive information and insights.

To learn more about how Alessa can help with your AML compliance activities, visit www.alessa.com

Cryptocurrency Intelligence with CipherTrace

CipherTrace develops cryptocurrency fraud prevention, anti-money laundering (AML), and, crypto compliance solutions based on leading cryptocurrency intellgence and the world's most block. Leading exchanges, banks, auditors, regulators and digital asset businesses use CipherTrace to comply with regulatory requirements, investigate financial crimes, and foster trust in the crypto economy.

CipherTrace Armada delivers deep insight into the fraud and money laundering risks from virtual asset service providers (VASPs). Powered by the worlds leading cryptocurrency intelligence and blockchain analytics, the Armada data feed enables bank customer due diligence (CDD) and transaction monitoring systems to become crypto-aware to help mitigate operational, legal, reputational and counterparty risks.

The CipherTrace Inspector financial investigations solution helps financial investitgators follow the money through the crypto economy. Even non-technical analysts and agents can use this powerful de-anonymization tools to easily identify and trace criminals who attempt to use any of more than 800 cryptocurrencies — including Bitcoin, Bitcoin Cash, Ethereum and Litecoin—on the internet to conceal their illicit activities. This de-anonymization capability spans more than 87% of global virtual assets.

CipherTrace Traveler helps Virtual Asset Service Providers comply with global "Travel Rule" regulations by securely sharing cryptocurrency transaction information with other vetted VASPs. It enables AML compliance and operational continuity in jurisdictions that enforce Travel Rule regulations by enabling secure exchange transaction confirmations.

About Alessa

Alessa is a compliance, controls monitoring and fraud prevention solution for banking, insurance, fintech, gaming, manufacturing, retail and more. With deployments around the world, Alessa allows organizations to quickly detect suspicious transactions, identify high-risk customers and vendors and decrease fraud risks that reduces profitability and increases costs. To learn more about how Alessa can help your organization ensure compliance to regulations, detect complex fraud schemes, and prevent waste, abuse and misuse, visit us at **https://www.alessa.com/.**

About CipherTrace

CipherTrace, the leading cryptocurrency intelligence company, bridges virtual currencies and financial services together with fraud protection, anti-money laundering, and financial crime prevention. CipherTrace derives superior cryptocurrency intelligence from analyzing massive amounts of validated blockchain transaction attribution and auditing VASP KYC thresholds. For more information, visit **https://CipherTrace.com/.**

150 Isabella Street, Suite 800,
Ottawa, ON K1S 1V7, Canada

1-844-265-2508

connect@alessa.com

www.alessa.com

ALESSA